UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/814,409	03/11/97	KITAJIMA H	826.1377/JPH

LM02/0717

STAAS & HALSEY
700 ELEVENTH STREET N W
SUITE 500
WASHINGTON DC 20001

EXAMINER	
MEISLAHN, D	
ART UNIT	**PAPER NUMBER**
2767	13

DATE MAILED: 07/17/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	Applicant(s)
08/814,409	Kitajima et al.
Examiner	**Group Art Unit**
Douglas Melslahn	2767

☒ Responsive to communication(s) filed on *Apr 10, 2000*

☒ This action is **FINAL.**

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *3* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claim

☒ Claim(s) *1-25* is/are pending in the applicat

Of the above, claim(s) _____ is/are withdrawn from consideration

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) *1-25* is/are rejected.

☐ Claim(s) _____ is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐ approved ☐ disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☒ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____.

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☐ Notice of References Cited, PTO-892

☐ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

— SEE OFFICE ACTION ON THE FOLLOWING PAGES —

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 10 April 2000 that amended claims 1, 10, and 19-25.

Response to Arguments

2. Applicant's arguments filed 10 April 2000 have been fully considered but they are not persuasive. The features added by the amendment are not part of the encryption or decryption circuit. Thus, interpreting the examiner's acknowledgement that "instructions to change the algorithm and the algorithm itself come from sources external to the circuit" to mean that an encryption apparatus does not include a change data generating unit is inappropriate. It is inherent that, for a change to occur, change data is produced. The maker of this information can be considered to be part of the encryption apparatus. The word automatic does not have any reference (data is generated automatically with respect to what?) and is therefore not treated.

3. Applicant ignores the basic teaching of Jovanovich et al., that is using compilers with digital memory.

4. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re*

Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, automation which increases efficiency provides a reason to combine the references.

In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., changing specifically the algorithm) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 21-22 are rejected under 35 U.S.C. 102(b) as being anticipated by Dabbish (4972478).

In the abstract, Dabbish discloses a ". . . logic cryptographic circuit that can be reprogrammed with various cipher algorithms." Reprogramming implies changing means. Changeable deciphering apparatus is mentioned in column 3, lines 44-46. Part 104 on Dabbish's diagram is communication circuitry, meaning that the apparatus can be connected to a communication network. In lines 51-67 of column one, Dabbish states that orders to change the encryption algorithm originate from sources external to the apparatus.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 5, 8, 10, 14, 17, 19, 20, and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish.

In the abstract, Dabbish discloses a " . . . logic cryptographic circuit that can be reprogrammed with various cipher algorithms." Reprogramming implies changing means. Changeable deciphering apparatus is mentioned in column 3, lines 44-46. Part 104 on Dabbish's diagram is communication circuitry, meaning that the apparatus can be connected to a communication network. In lines 51-67 of column one, Dabbish states that orders to change the encryption algorithm originate from sources external to the apparatus. Dabbish does not say that the structure of the algorithms is changed. Official notice is taken that cryptographic hardware is faster than cryptographic software. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to make the programmability of Dabbish based upon hardware modification in order to achieve greater speed.

9. Claims 2-4, 6, 11-13, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish in view of Jovanovich et al. (5703950).

Dabbish presents a system in which ciphering algorithms are written to a circuit, thus changing the algorithm that the circuit follows. The instructions to change the

algorithm and the algorithm itself come from sources external to the circuit. Dabbish does not disclose configuration means, a compiler, libraries, databases, or mapping data objects. He further does not disclose that the cipher algorithm is encrypted. Official notice is taken that it is old and well-known to encrypt data so as to prevent it from being used by parties other than the intended recipient. Official notice is also taken that object oriented programming is old and well-known. In lines 58-64 of column 3, Jovanovich et al. talk about storing data in a database. The data is compiled by configuration means. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to store cipher algorithms in a database from which configuration means would compile an algorithm and write it, as an object, to the circuit. In object-oriented programming, libraries containing data are common. It would also be obvious to encrypt data that is sent to the circuit. This would protect the data, foiling those who would otherwise have intercepted the data and created their own identical circuit. It would also act to disallow sending false data to the circuit. Data that was not encrypted according to a key in the circuit would not create an intelligible algorithm. Finally, it would protect the new circuit specifications while minimizing use of keys used to decrypt messages. This advantage is similar to the advantages of session key use as opposed to master key use.

10. Claims 7 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish.

Dabbish presents a system in which ciphering algorithms are written to a circuit, thus changing the algorithm that the circuit follows. The instructions to change the

algorithm and the algorithm itself come from sources external to the circuit. Dabbish does not say that the algorithms are updated on a periodic basis. Official notice is taken that updating keys or other cryptographic devices is old and well-known. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to allow for periodic updates of the circuit, making it particularly useful in time specific applications such as pay television systems.

11. Claims 9 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Dabbish in view of Lynn et al. (5345508).

Dabbish presents a system in which ciphering algorithms are written to a circuit, thus changing the algorithm that the circuit follows. The instructions to change the algorithm and the algorithm itself come from sources external to the circuit. Dabbish does not mention changing the circuits specifications based upon the communication path, degree of communication path security, or the process speed required. Lynn et al. talk about changing encryption keys based upon processing time and security. They specifically describe how their invention can be used to balance these factors in the first paragraph of the brief summary, line 54 of column 2 through line 36 of column 3. Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to allow for changes in the circuits specifications based upon the communication path, degree of communication path security, or process speed required. This would give flexibility to the system, letting it adapt to security and speed requirements.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached between 9AM - 6PM, except for every other Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann can be reached on (703) 308-7791. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 308-9051 for regular communications and (703) 308-9052 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Douglas J Meislahn
Examiner
Art Unit 2767

DJM
July 12, 2000